PRV
PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* *Solid AB, Stockholm SE*
Applicant (s)

(21) *Patentansökningsnummer* *0302733-1*
Patent application number

(86) *Ingivningsdatum* *2003-10-16*
Date of filing

Stockholm, 2004-10-14

För Patent- och registreringsverket
For the Patent- and Registration Office

Gunilla Larsson

Avgift
Fee

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

LOCK SYSTEM

FIELD OF INVENTION

The present invention relates generally to lock systems and more particularly to a lock system which can be set up in an easy and yet secure way and be operated with a high security level.

BACKGROUND

Electronic or electro-mechanical lock systems having locks or the like that are connected to a central computer or system by means of a cable network have been in use for many years. The operation of these systems are managed from the central computer which communicate the applicable rules via a local network (LAN) to individual door access control (DAC) units. The DAC units in turn communicate e.g. log information to the central computer.

It is of vital importance that the communication between the central computer and the individual DAC units is secure, i.e., that it cannot be intercepted and interpreted or manipulated by a fraudulent person trying to gain unauthorized access to the premise in which the lock system is installed.

In prior art lock systems this high level of security has been achieved by the use of proprietary communication protocols, shielded communication wires etc. However, today's users are not prepared to install a separate protected cable network for a lock system in parallel with a computer network already installed in

the office, such as an Ethernet based network, or to use proprietary systems tying them to one or a limited number of suppliers.

One way of achieving secure communication on a pre-existing network is to use encrypted data for communication between the central computer and the individual DAC units. However, before using encrypted communication, the different units communicating must have encryption/decryption keys installed. These keys could be installed by skilled personnel that provide each and every unit with the required keys. One problem associated with this solution is that the persons normally installing such lock systems are not skilled personnel in the sense that they are not familiar with computer hardware and software. Thus, installation of encryption/decryption keys would be performed by expensive personnel in a separate step after the physical installation of the system, leading to increased costs. Also, the use of individuals for installing software is a security risk in itself.

A problem in prior art is thus to provide a lock system which shows a high degree of security while the installation and set-up of the system can be effected in an easy way.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a lock system wherein the prior art drawbacks are avoided and in which encryption keys can be installed in an easy and yet secure way. This means that one specific object is

that installation of components must be as simple as possible.

Another object is that security breach by customer mistakes must not affect other customers or the manufacturer.

Yet another object is to provide a system and method wherein existing standards and implementations are used as much as possible.

Still yet another object is to provide a method wherein system requirements are kept as small as possible.

The invention is based on the realisation that the use of certificates in combination with asymmetric and symmetric encryption in a lock system provides a secure yet efficient solution to the above described problem.

According to the invention there are provided method of installing a lock system as defined in claim 1 and a lock system as defined in claim 9.

By providing a lock system which is set up by means of both asymmetric and symmetric communication between the units in the system both simple installation and high security are achieved.

In a particularly preferred embodiment, a unique symmetric encryption key is used for each door access control unit. This ensures that the integrity of the lock system is maintained in the case one or more of the DAC units are taken over by a fraudulent person trying to gain unauthorized access to the premise in which the lock system is installed.

Further preferred embodiments are defined by the dependent claims.

BRIEF DESCRIPTION OF DRAWINGS

The invention is now described, by way of example, with reference to the accompanying drawings, in which:

fig. 1 is an overall view of a the hardware including a manufacturer and customer lock systems;

fig. 2 is a block diagram showing a Public Key Infrastructure implemented in the lock system according to the invention;

fig. 3 is a simplified diagram showing the different steps in the method according to the invention; and

fig. 4 is a detailed diagram showing the different steps in the method according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following a detailed description of a preferred embodiment of the present invention will be given.

In the present description, the term "lock system" is intended to cover all types of electronic lock systems wherein the door access units control electronic or electro-mechanical locks, card readers, panic buttons etc. (not shown in the figures) and is thus not limited to systems comprising conventional lock cylinders or the like.

An environment in which the present invention is implemented will now be described with reference to figure 1. It is there shown a manufacturer computer

system 10, which comprises computer hardware with peripherals etc. and access to the Internet. The manufacturer computer system runs software adapted for processing of customer certificates. The management system is divided into a front end system that collects signature request and a back end system that holds the manufacturer's private key used for signing of a customer public key. The subsystem that contain the private key responsible for signing customers' certificate is not exposed to public networks .

A number of customer lock systems, generally designated 100, two of which are shown in the figure, each comprises a customer management computer 110 connected to a plurality of door access control (DAC) units 120 via a local area network (LAN) 130. The LAN could be Ethernet-based but the invention does not exclude other kinds of networks.

The management computer 110 is the computer wherein all rules relating to the lock system 100 is managed and stored. These rules can be related to which individuals are authorised to open which doors, temporal restrictions to access to doors etc. These rules are downloaded to the individual DAC units 120 which effect the physical control of the doors by means of actuators etc.

The present invention uses the well-known Public Key Infrastructure (PKI) which uses techniques for public-key encryption, also referred to as asymmetric encryption. In public-key encryption systems each entity has a public key and a corresponding private key. The

public key defines an encryption transformation, while the private key defines the associated decryption transformation. Any entity wishing to send a message to another entity A obtains an authentic copy of A's public key, uses the encryption transformation to obtain the cipher text, and transmits this cipher text to A. To decrypt the cipher text, A applies the decryption transformation to obtain the original message.

The public key need not be kept secret, and, in fact, may be widely available – only its authenticity is required to guarantee that A is indeed the only party who knows the corresponding private key. A primary advantage of such systems is that providing authentic public keys is generally easier than distributing secret keys securely, as required in symmetric key systems.

Since A's encryption transformation is public knowledge, public-key encryption alone does not provide data origin authentication or data integrity. Such assurances must be provided through use of additional techniques, including message authentication codes and digital signatures. Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms.

Public-key decryption may also provide authentication guarantees in entity authentication and authenticated key establishment protocols.

The Public Key Infrastructure in a lock system according to the invention will now be described with reference to fig. 2, wherein part of the environment shown in fig. 1 is detailed. More specifically, the manufacturer

computer system 10, a management computer 110, and a DAC unit 120 are shown therein, but not the physical interconnections (the Internet, LAN). It is here seen that the manufacturer functions as an upper level Certificate Authority - CA level 1 - and the lock system owner as a lower level CA – CA level 2. To achieve a scalable installation of the DAC units 120 and to restrict problems of a comprised management computer to a customer domain, part of the PKI have been arranged as this hierarchy.

The installation procedure for the lock system shown in fig. 1 will now be explained in detail with reference to fig. 3, which shows the major steps of the procedure, and fig. 4, which is a more detailed representation.

As a first step, the manufacturer public key is installed in the DAC unit at a trusted factory. A security feature is boot-strapped into the DAC units in the form of a certificate trusting the manufacturer's software. This means that the DAC units' software can only be installed under the manufacturer's control.

Each and every DAC unit 120 is thus provided with the manufacturer public key. This is a more efficient and reliable way than providing the public key when the DAC unit already has been installed. This method also provides DAC units that are essentially identical before delivery, facilitating logistics and storage. Optionally, each DAC unit is provided with a unique serial number. However, this is not important for the present invention.

When a DAC unit boots for the first time it retrieves the installer program image, checks the signature against the factory installed manufacturer public key and starts to execute upon match. The temporary installer application is capable of verifying the manufacturer's signature of the customer's public key and could verify that the certificate presented by the management computer 110 has been signed by the manufacturer computer 10. The manufacturer public certificate is bundled with the installer image, which is signed by manufacturer private key.

Because the DAC units only trust the manufacturer at delivery, the customers do not have full control over their own system, which in their view is unacceptable. Each customer wants control of its own system. Therefore, the customer receives a certificate signed by the manufacturer. This certificate is delivered on-line through a procedure, wherein the receiver is obliged to identify himself or herself. More specifically, the receiver is indicated in the certificate as attributes. This ensures that a specific individual is responsible, increasing the security level of the inventive concept.

The certificate signed by the manufacturer is used in a further step to install a certificate trusting the customer. In that way, the customer gets full control of the system except for software updating, see below.

When a lock system owner buys the management computer software and obtains media together with a unique code, the name of the lock system owner is registered in the manufacturer computer 10 together with the software

version. The lock system owner is then instructed to contact the manufacturer to get its management computer public key signed by the manufacturer, i.e., the upper level CA. The lock system owner's management computer public certificate is then added in a database located in the manufacturer computer 10.

When the lock system owner installs the lock system software or when the lock system 100 is about to be set up, the management computer 110 generates a symmetric encryption key pair and makes available the certificate signed by the manufacturer. In that way, the management computer 110 becomes a CA of itself.

After having been connected to the LAN 130, when the DAC unit 120 is turned on, the installer program image that has been installed in the DAC unit accepts the management computer public certificate signed by the manufacturer. An encrypted and authenticated channel is then established, such as by means of an SSL-session using asymmetric encryption, between the management computer and the DAC unit. By means of this communication channel, the DAC unit then installs the symmetric secret key from the management computer. From this moment asymmetric methods are replaced by symmetric by terminating the asymmetrically encrypted channel and establishing a symmetrically encrypted tunnel and the DAC unit could thereafter only be controlled by the management computer to prevent hostile takeover from other management computer systems.

In the preferred embodiment, the factory installed manufacturer public key remains in the DAC unit to

verify software from the manufacturer. This prevents customers to remote install unauthorized software in the DAC unit.

After the set-up of the lock system 100 has been completed, further communications between the management computer 110 and the DAC 120 are effected by means of symmetric encryption. A unique symmetric encryption key is used for each DAC unit, i.e., the management computer uses different symmetric encryption keys for the DAC units. This ensures that the integrity of the lock system is maintained in the case one or more of the DAC units are taken over by a fraudulent person trying to gain unauthorized access to the premise in which the lock system is installed.

Asymmetric encryption is more demanding on hardware, which is inconvenient when taking hardware costs into consideration. This is one reason why the lock system according to the invention operates in a secure yet efficient way.

It has been described how the manufacturer public key is distributed on-line. However, the manufacturer public key can also be distributed on compact disc, for example, when the software product is purchased.

Further communication between the manufacturer and the customer can be on-line by means of the Internet, for example, or by means of other media, such as compact disks.

In the described embodiment, the receiver of the manufacturer certificate is indicated as attributes in

the certificate. As an alternative, each certificate has a unique serial number distinguishing it from other certificates. It is also preferred that the certificate is protected by means of some kind of password, such as a PIN code.

A preferred embodiment of a lock system according to the invention has been described. A person skilled in the art realises that this could be varied within the scope of the appended claims.

The manufacturer computer system and management computers have been described as interconnected via the Internet. It will be appreciated that some of the management computers are not connected to the outside. In that case communication between the manufacturer computer system and management computers can be effected via other media, such as diskettes, compact discs etc.

For ease of understanding, the manufacturer computer system has been described as one single computer. It will be appreciated that there can be more than one computer at the manufacturer having different functions.

CLAIMS

1. A method of configuring a lock system (100) owned by a lock system owner and comprising a management computer (110) connected to a plurality of door access control units (120), said method comprising the following steps:

a) installing in the door access control units a first certificate issued by a manufacturer (10) of the lock system;

b) providing at the management computer (110) a second certificate issued by the lock system owner and signed by the manufacturer;

c) transmitting from the management computer to a first door access control unit of the door access units the signed second certificate together with a symmetric encryption key used by the lock system owner;

d) installing by means of asymmetric encryption the second certificate at the first door access control unit after checking the authenticity of the signed second certificate; and

e) establishing of symmetric encryption communication between the management computer and the first door access unit.

2. The method according to claim 1, wherein a unique symmetric encryption key is used for each door access control unit.

3. The method according to claim 1 or 2, wherein the step of installing a first certificate is performed under the control of a boot strapped security feature in the door access control unit.

4. The method according to any of claims 1-3, wherein the step of providing at the management computer a second certificate is performed on-line through a procedure, wherein a receiver identifies himself or herself.

5. The method according to claim 4, wherein the identity of the receiver is indicated in the second certificate as attributes.

6. The method according to any of claims 1-5, wherein the step of providing a second certificate comprises providing a symmetric encryption key pair.

7. The method according to any of claims 1-6, wherein the step of transmitting from the management computer to a first door access control unit the signed second certificate is preformed as an SSL-session.

8. The method according to any of claims 1-7, wherein the step of installing the second certificate involves keeping the first certificate so as to verify data from the manufacturer.

9. A lock system (100) owned by a lock system owner and comprising a management computer (110) connected to a plurality of door access control units (120),

characterized by

- a first certificate issued by a manufacturer (10) of the lock system provided in the door access control units (120);
- a second certificate issued by the lock system owner and signed by the manufacturer provided in the management computer (110);
- a symmetric encryption key pair provided in the management computer and a respective door access control unit (120); and
- a public asymmetric encryption key for the manufacturer provided in the door access control units.

10. The lock system according to claim 9, wherein a unique symmetric encryption key is provided for each door access control unit.

ABSTRACT

A lock system (100) is owned by a lock system owner and comprises a management computer (110) connected to a plurality of door access control units (120). A method of configuring this system comprises the following steps: installing in the door access control units a first certificate issued by a manufacturer (10) of the lock system; providing at the management computer (110) a second certificate issued by the lock system owner and signed by the manufacturer; transmitting from the management computer to a first door access control unit of the door access units the signed second certificate together with a symmetric encryption key used by the lock system owner; installing by means of asymmetric encryption the second certificate at the first door access control unit after checking the authenticity of the signed second certificate; and establishing of symmetric encryption communication between the management computer and the first door access unit. Simple yet secure installation of the lock system is thereby achieved.

(FIG. 1)

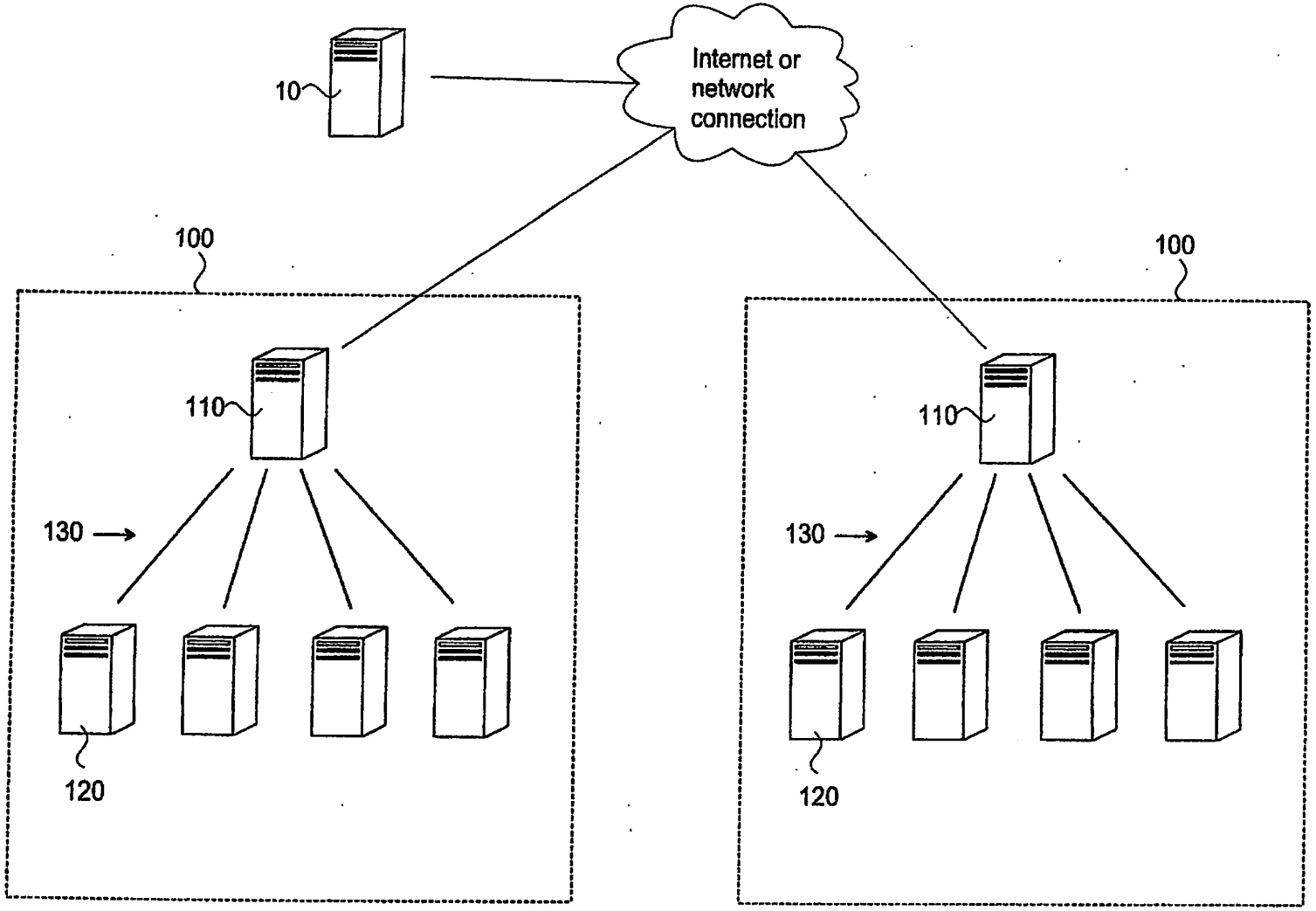
10
Internet or
network
connection
100
110
130
120
100
110
130
120

Fig. 1

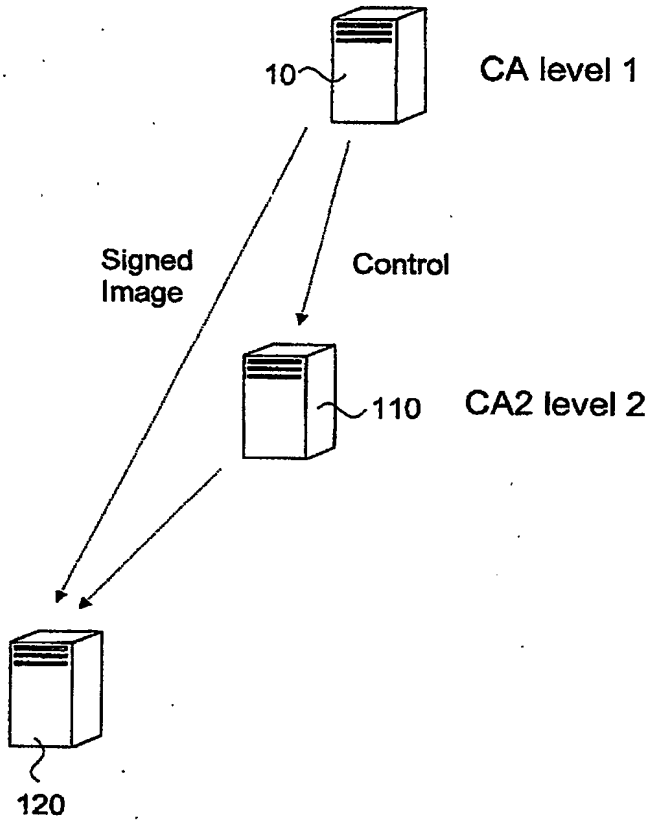

Fig. 2

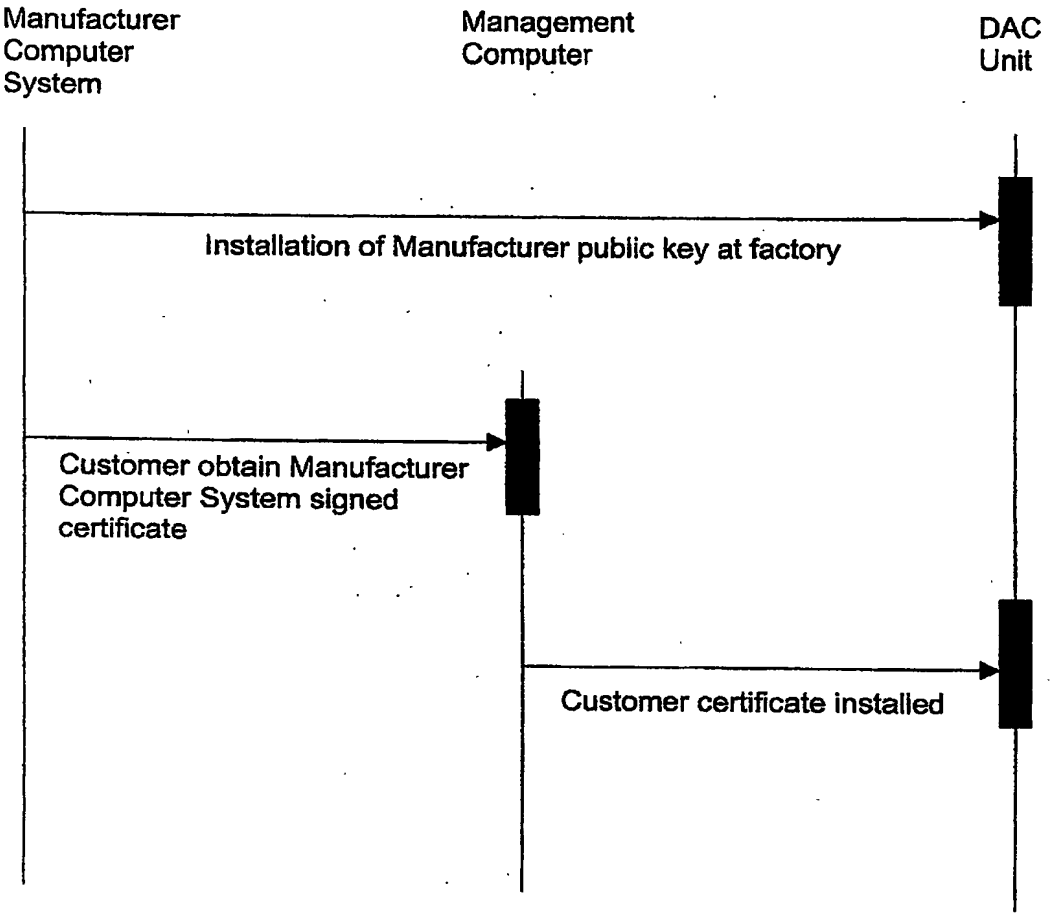

Fig. 3

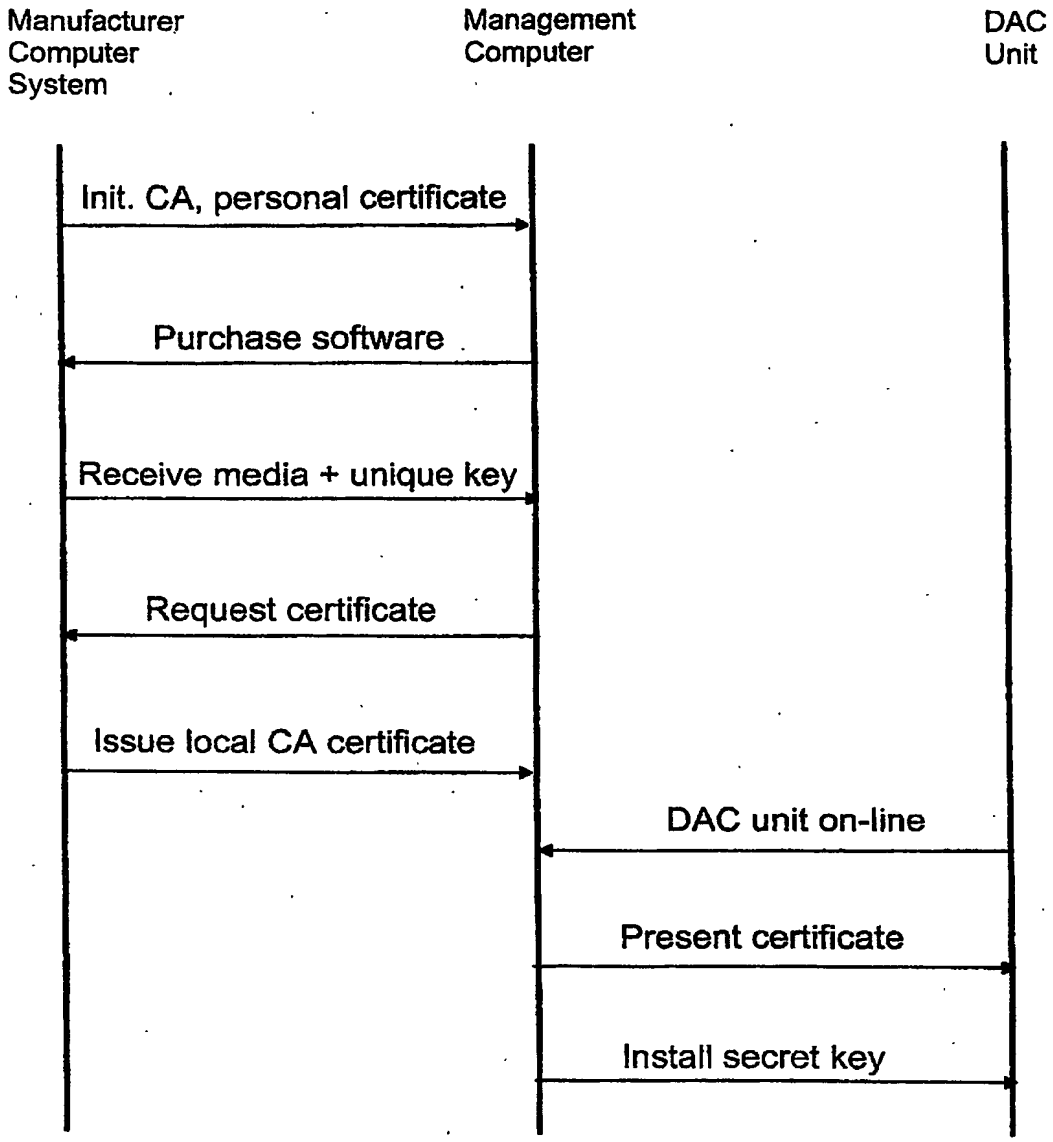

Fig. 4